UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,178	12/31/2003	Ariel Peled	27153	5563

67801 7590 11/01/2010

MARTIN D. MOYNIHAN d/b/a PRTSI, INC.
P.O. BOX 16446
ARLINGTON, VA 22215

EXAMINER	
GYORFI, THOMAS A	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
11/01/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/748,178	**Applicant(s)** PELED ET AL.
	Examiner Thomas Gyorfi	**Art Unit** 2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2010*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-61,63-80,107-130 and 147-149* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-61, 63-80,107-130 and 147-149* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-61, 63-80, 107-130 and 147-149 remain for examination. The amendment filed 9/2/10 added claim 149; amended claims 1, 73, 107, 110, and 130; and cancelled claim 62.

Response to Arguments

2. Applicant's arguments filed 9/2/10 have been fully considered but they are not persuasive. Applicant argues,

> The Examiner, in rejecting claim 62, cites a passage from Ginter column 43 line 55 - column 44 line 15, but the passage specifies that the user can *only* set a method *that does not conflict* with any existing method.
>
> Since Ginter sets up a situation in which the policies *cannot* conflict, it is clear that the skilled person considering Ginter has *no motivation* to try and solve the problem of what to do when policies *do contradict*.
>
> Hence it would not be obvious for the skilled person considering Ginter to solve the problem in the way defined by the amended claim, that is by selecting the stricter of the two policies.
>
> Furthermore, since in Ginter the policies cannot conflict *ab initio,* the skilled person starting with Ginter has *no motivation to search in other art* for a solution to the problem. That is to say the skilled person has no motivation to solve a problem that is *explicitly taught not to arise.*

To the best of Examiner's understanding, Applicant appears to be arguing that security policy conflicts do not occur in the Ginter invention simply because they cannot occur from the outset; but what Applicant has failed to consider is that in order for there not to be any conflicting VDE control information objects (i.e. the security policies) in the Ginter invention, it must first be able to recognize when someone is attempting to break the system through the creation of an invalid policy in the first place. For example, consider an exemplary piece of content produced by a content owner/creator and protected by VDE control information that sets specific limits as to what can be done with said content (see Ginter, col. 44, lines 15-30). Another party, perhaps either the content distributor or the end user, may attempt to create new VDE control information, using whatever aspect of Ginter's invention would be required to do so (Ibid, and Ginter, col. 44, lines 1-15). Examiner assumes *arguendo* that said another party may try to establish new permissions that are less restrictive than those explicitly granted by the original content creator in an attempt to circumvent the disclosed system, even though one of ordinary skill in the art would have no reason to expect that e.g. an end user could or should override the wishes of the content creator/copyright holder. Therefore, when an entity further down the distribution chain creates an additional VDE control information object, there will exist for at least a brief moment in time in the Ginter computer's memory at least two VDE information objects pertaining to the same piece of content: the original one from the content creator and the more permissive object from the other party. Thus the Examiner understands the pertinent portions of Ginter to teach that in the event that this scenario were to occur, the Ginter invention will discard the newer, more permissive VDE control information object in favor of the more restrictive policy initially set by the content creator, to resolve the conflict immediately rather than allow it to needlessly persist to some unknown future point in time. In view of the above, Examiner respectfully submits that the only context that Applicant's overly literal analysis of Ginter would make sense would be if Ginter were to rely on the honor system for conflict resolution - i.e. conflicts cannot occur merely because no one would ever even try to create a VDE control object that could conflict with a pre-existing VDE control object. If that were true, it would logically lead to an egregiously obvious loophole in the protection ostensibly afforded by Ginter’s invention, as one could override any security by creating a new VDE control object that grants oneself full access to protected content, and thus render the Ginter invention as unfit for its stated purpose. Since Ginter must have some means to prevent that absurdity from occurring, it follows that whatever means Ginter employs – as implied from the previously cited passage(s) – must read on the disputed limitation.

3. Examiner would also like to point out that the disputed limitation of the independent claims is, in the Examiner’s purview, an aspect of what those of ordinary skill in the art of computer security know well as the "principle of least privilege". To wit, one would have readily understood that as a general rule the idea that an entity should only have the minimum level of security access/privilege that one requires to accomplish one's task(s), and no more; thus in a situation where conflicting security policy information might confuse the issue of what rights a user might have to a particular piece of content, those of ordinary skill in the art could have easily applied the principle of least privilege to the situation to determine that the most restrictive policy is likely the best, absent extenuating circumstances to the contrary. Additional references attesting to the general obviousness of this limitation are enclosed herein.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-61, 63-80, 107-130, and 147-149 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al (U.S. Patent 5,892,900) in view of Gilmour (U.S. Patent 6,205,472).

Regarding claims 1, 110, and 149:

Ginter discloses a method and system for computer workstation based information protection, comprising: monitoring user's actions on said computer workstation (col. 1, lines 20-30); analyzing said monitored action in respect to a predefined policy associated with any confidential information identified by said analysis as being associated with said content in use at said workstation, to determine whether said actions prejudice information to which the policy applies (col. 302, line 40 – col. 303, line 40); and executing said policy in accordance with the results of said analysis to control said actions (Ibid), and wherein in the event of two or more conflicting policies are found, a strictest one of the policies is identified and used (col. 43:55 – col. 44:30).

Although Ginter discloses using statistics and statistical analysis in the disclosed system (col. 105, lines 15-50), it appears to be silent regarding using the statistical analysis for the specific purpose of identifying confidential information. However, Gilmour discloses a general technique for data management using statistical analysis with a number of identifiers to determine within a given confidence level if confidential information is present (the second matching step of col. 2, lines 20-50; identifiers at col. 13, lines 15-25; more detail at col. 21, lines 10-50). The claims are thus obvious because the ability to use statistical analysis to identify confidential data was a technique that was within the capabilities of one of ordinary skill in the art, in view of its teaching for improvement in similar situations.

Regarding claims 2 and 111:

Ginter further discloses wherein said policy comprises restrictions on at least one of: print, save, copy, autosave, fax (col. 252, line 40 – col. 253, line 30).

Regarding claims 3 and 112:

Ginter further discloses wherein said monitoring said user's actions on said workstation computer comprise detection of indications of attempts of tampering (col. 85, lines 45-57).

Regarding claim 4:

Ginter further discloses obtaining logical indications or statistical indications (Ibid, and col. 88, lines 10-50).

Regarding claims 5 and 113:

Ginter further discloses detection of at least one uncertified add-in (col. 85, lines 45-65, noting that uncertified add-ons would not be validated).

Regarding claim 6:

Ginter further discloses noting that said uncertified add-in is hooked to event of a local operating system (Ibid).

Regarding claims 7 and 114:

Ginter further discloses detection of at least one debugging technique (col. 88, lines 10-50).

Regarding claim 8:

Ginter further discloses wherein said debugging technique comprises any of a debugger, virtual machine, software emulator, software trap, and remote administration tool (Ibid).

Regarding claims 9 and 115:

Ginter further discloses wherein said policy comprises restrictions of actions made available to said user upon detection of indications of attempts of tampering (col. 176, lines 5-20).

Regarding claims 10 and 116:

Ginter further discloses applying restrictions on actions within a software application operable to process said information (col. 308, line 40 – col. 307, line 5).

Regarding claim 11:

Ginter further discloses performing at least one action upon detection of indications of attempts at tampering (col. 205, lines 40-60).

Regarding claim 12:

Ginter further discloses at least one of encrypting at least one buffer, and encrypting at least one shared memory (col. 199, line 33 – col. 200, line 22).

Regarding claim 13

Ginter further discloses wherein said actions comprise preventing the decryption of encrypted digital content (col. 205, lines 40-60).

Regarding claim 14:

Ginter further discloses wherein said pre-defined policy is defined with respect to a software application on said user's workstation (col. 311, lines 30-60).

Regarding claim 15:

Ginter further discloses wherein said policy comprises reporting about attempts to perform actions that do not comply with an organization policy or are suspected to not comply with the organizational policy (col. 145, lines 25-50).

Regarding claim 16:

Ginter further discloses wherein said policy comprises performing logging of attempts to perform actions that do not comply or are suspected to not comply with the organizational policy (Ibid).

Regarding claim 17:

Ginter further discloses protecting information held within a software data processing application able to process said information (col. 308, line 40 – col. 307, 5).

Regarding claim 18:

Ginter further discloses wherein said software data processing application operates in conjunction with a software client (Ibid).

Regarding claims 19 and 117:

Ginter further discloses wherein said software client is tamper resistant (col. 87, line 60 – col. 88, line 10).

Regarding claims 20 and 118:

Ginter further discloses wherein said software client is operable to monitor a user's actions and to execute said policy (col. 307, lines 1-5).

Regarding claims 21 and 119:

Ginter further discloses wherein said software client is operable to monitor said user's actions and policy (Ibid).

Regarding claims 22 and 120:

Ginter further discloses wherein said software client is further operable to detect events of said software application (col. 42, lines 15-40).

Regarding claim 23:

Ginter further discloses wherein said events comprise any of: printing, copying storing, and displaying said information (col. 251, line 60 – col. 252, line 40).

Regarding claims 24 and 121:

Ginter further discloses wherein said policy further comprises managing usage rights (col. 33, lines 35-65).

Regarding claim 25:

Ginter further discloses wherein said usage rights are determined according to any of the classification of the document, the classification level of the user, and the authentication level of the user (col. 302, lines 50-55).

Regarding claims 26 and 122:

Ginter further discloses wherein the usage rights comprise any of viewing at least part of said information; modifying at least part of said information; sending at least part of said information to a recipient; storing at least part of said information; storing at least part of said information by an application; storing at least part of said information by a file system; storing at least part of said information in a portable device;storing at least part of said information in a removable media; storing at least part of said information portable storage device that is connected to said workstation using a USB port; pasting at least part of said information into a document; printing at least part of said information; printing at least part of said information to file; printing at least part of said information to a fax, and printing a screen view document (col. 156, line 60 – col. 157, line 20).

Regarding claim 27:

Ginter further discloses wherein said policy comprises definition of actions to be performed (col. 189, line 40 – col. 190, line 35).

Regarding claim 28:

Ginter further discloses wherein said actions comprise any of: enabling usage of at least part of said information, disabling usage of at least part of said information; restricting usage of at least part of said information according to a pre-determined set of restrictions; reporting about the usage of at least part of said information, and monitoring the usage of at least part of said information (Ibid).

Regarding claim 29:

Ginter further discloses wherein restriction of usage imposes requiring encryption of at least part of said protected information (col. 14, lines 25-50).

Regarding claim 30:

Ginter further discloses wherein said required encryption is such that corresponding encrypted information can be decrypted only by a secure client (Ibid).

Regarding claim 31:

Ginter further discloses wherein said restriction of usage requires said protected information to reside on a secure server (col. 106, lines 40-55).

Regarding claim 32:

Ginter further discloses arranging a connection between said secure server and said workstation such that the transport between said secure server and said workstation is protected (col. 12, lines 30-40).

Regarding claim 33:

Ginter further discloses wherein said protected transport comprises encrypted transport (Ibid).

Regarding claim 34:

Ginter further discloses encryption of a file comprising at least part of said protected information wherein said file is at least one of the following: temporary file and auto-recovery file (col. 173, lines 13-67).

Regarding claim 35:

Ginter further discloses a file comprising at least part of said protected information, wherein said file comprises any of temporary file and auto-recover file (Ibid).

Regarding claim 36:

Ginter further discloses wherein said software client authenticates itself to a server before at least some of the sessions (col. 36, lines 10-45; col. 168, lines 45-67).

Regarding claim 37:

Ginter further discloses wherein said authentication depends on a classification level assigned to protected information (col. 302, lines 50-55).

Regarding claim 38:

Ginter further discloses wherein authentication is any of password based or network address based (col. 199, lines 5-10).

Regarding claim 39:

Ginter further discloses wherein said software client comprises components that can be automatically replaced (col. 16, lines 1-20).

Regarding claim 40:

Ginter further discloses wherein said secure server employs cryptographic encryption of at least one file containing said protected information (col. 37, lines 45-55).

Regarding claim 41:

Ginter further discloses wherein communication with said server is substantially transparent to said user (col. 34, lines 40-50).

Regarding claim 42:

Ginter further discloses wherein in accordance with said policy said protected information is encrypted utilizing the encryption capabilities of said software application (col. 22, lines 1-5).

Regarding claims 43 and 125:

Ginter further discloses wherein said software application operable to process said information is a word processing application (col. 301, lines 30-40).

Regarding claim 44:

Ginter further discloses wherein said software application comprises a control flag imparting the status of either read only or lock to a corresponding file, and wherein file modification within said software application which is operable to process said information is disabled via said flag (col. 247, lines 50-57).

Regarding claim 45:

Ginter further discloses wherein said disabling of said file modification is controlled by said policy (Ibid).

Regarding claim 46:

Ginter further discloses wherein said policy comprises adding forensic information to said protected information (col. 201, line 45 – col. 202, line 5).

Regarding claims 47 and 126:

Ginter further discloses wherein said software client replaces the clipboard functionality of said software application thereby to process said protected information with a secure clipboard functionality (col. 323, lines 10-55).

Regarding claim 48:

Ginter further discloses wherein said protected information copied into said secure clipboard is stored in an internal data structure inaccessible to other applications (Ibid).

Regarding claims 49 and 127:

Ginter further discloses wherein said software client is installed automatically from a remote server (col. 237, lines 20-40).

Regarding claims 50 and 128:

Ginter further discloses wherein said installation of said software client utilizes anti-virus installation infrastructure (col. 240, lines 15-42).

Regarding claim 51:

Ginter further discloses wherein updates of said software client utilizes anti-virus installation infrastructure (Ibid).

Regarding claim 52:

Ginter further discloses wherein at least part of the software code of said software client resides in an encrypted form (col. 237, lines 20-40).

Regarding claim 53:

Ginter further discloses wherein at least part of the software code of said software client is attached to hardware of said computer workstation (col. 87, 5-30).

Regarding claim 54:

Ginter further discloses wherein said software client is operable to automatically add information to said protected information in accordance with said policy (col. 201, line 45 – col. 202, line 5).

Regarding claim 55:

Ginter further discloses wherein said added information comprises any of a document header, footer, or textual disclaimer (col. 135, lines 20-35).

Regarding claim 56:

Ginter further discloses wherein said software client is operable to open file that comprises said protected information only while connected to at least one server (col. 109, lines 20-67).

Regarding claim 57:

Ginter further discloses wherein said servers enforce policy with respect to said information (col. 302, lines 40-60).

Regarding claim 58:

Ginter further discloses wherein said policy implies a set of restrictions regarding the usage of said protected information (col. 214, lines 15-40).

Regarding claim 59:

Ginter further discloses wherein the client software is operable to check that it is connected to a predetermined server before decrypting a file that comprises protected information (col. 109, lines 20-67).

Regarding claim 60:

Ginter further discloses wherein said servers enforce a policy with respect to said protected information, and wherein said policy comprises a set of restrictions regarding the usage of said protected information (col. 214, lines 15-40).

Regarding claim 61:

Ginter further discloses wherein at least two servers are operable to define said policy (col. 307, lines 25-55).

Regarding claim 63:

Ginter further discloses wherein in the event of two or more conflicting policies are found, a union of the policies is identified and used (Ibid).

Regarding claim 64:

Ginter further discloses wherein connection to at least two servers are required in order to determine policy (col. 307, lines 25-55).

Regarding claim 65:

Ginter further discloses wherein said server authenticates the integrity of said client by requiring a cryptographic hash of at least part of said client’s software (col. 223, lines 45-67).

Regarding claim 66:

Ginter further discloses wherein said cryptographic hash is with respect to a random address in said client’s software (col. 131, line 27 – col. 132, line 13).

Regarding claim 67:

Ginter further discloses wherein said client is entangled with said server's software, such that a functioning stand-alone copy of said client's software does not exist (col. 103, lines 45-67).

Regarding claim 68:

Ginter further discloses wherein said method comprises at least two levels of protection, and wherein said levels of protection are operable to be configured as a function of the secrecy of said protected information (col. 302, lines 50-55).

Regarding claim 69:

Ginter further discloses wherein in the most secure of said levels of protection, said protected information can only be accessed while connected to said server (col. 103, lines 45-67).

Regarding claim 70:

Ginter further discloses wherein in at least one of said levels of protection, said information can be accessed for a limited time after the connection with said server was terminated (col. 32, lines 50-60).

Regarding claim 71:

Ginter further discloses wherein at least one of said levels of protection, said information can be accessed until the end of a current login session (col. 103, 45-67).

Regarding claim 72:

Ginter further discloses wherein in at least one of said levels of protection, said information can be unlimitedly accessed after the server approves the information (col. 198, lines 50-60).

Regarding claims 73 and 130:

Ginter discloses a method and system for information protection comprising: defining an information protection policy with respect to an information item, said defining comprising at least one measure, required to be enforced by said workstation, in said policy to protect said information item (col. 300, lines 40-50; workstations at col. 303, lines 40-50); and allowing usage on a computer workstation of content comprising said information item only while required measures in said policy are being applied by said workstation (col. 302, line 40 – col. 303, line 40); and wherein in the event of two or more conflicting policies are found, a strictest one of the policies is identified and used (col. 43, line 55 – col. 44, line 30).

Although Ginter appears to disclose the use of identifiers from a content identifier database to identify protected information items (such as traveling objects: see col. 138, lines 43-62; and col. 305, line 45 – col. 306, line 5), Ginter does not explicitly disclose the use of statistical analysis in the process. However, Gilmour discloses a general technique for data management using statistical analysis with a number of identifiers to determine within a given confidence level if confidential information is present (the second matching step of col. 2, lines 20-50; identifiers at col. 13, lines 15-25; more detail at col. 21, lines 10-50). The claims are thus obvious because the ability to use statistical analysis to identify confidential data was a technique that was within the capabilities of one of ordinary skill in the art, in view of its teaching for improvement in similar situations.

Regarding claim 74:

Ginter further discloses protecting information with a client software application (col. 26, lines 35-65).

Regarding claim 75:

Ginter further discloses disabling at least one of the controls of said application (e.g. disabling the print ability when a document should not be printed: col. 250, line 40 - col. 251, line 18).

Regarding claim 76:

Ginter further discloses wherein said information protection measures comprise encryption of the memory of a graphic card or video card (col. 250, line 40 – col. 251, line 60, but particularly col. 250, lines 52-55 and col. 251, lines 30-40).

Regarding claim 77:

Ginter further discloses wherein said information protection measures comprises forcing a video card or a graphic card to a mode that causes no meaningful information to be stored in said video card's memory (an *encrypted* VDE-object in the graphics card memory is meaningless without the ability to decrypt, which an attacker would not be able to do: Ibid).

Regarding claim 78:

Ginter further scanning at least one storage device and identifying the existence of pre-defined information objects (i.e. using a VDE for document control: col. 302, lines 15-40; VDE-enabled storage devices at col. 250, lines 40-60).

Regarding claim 79:

Ginter further discloses wherein said pre-defined objects comprise confidential information objects (col. 302, lines 50-55).

Regarding claim 80:

Ginter further discloses at least one rule regarding at least one event of at least one software application operable to handle said information (e.g. a printing rule applied to a VDE-enabled word processor: col. 26, lines 35-65).

Regarding claim 107:

Ginter discloses a method for computer workstation based information protection, comprising: detecting an event occurring at said workstation, said event being associated with content (col. 42, line 17 – col. 43, line 20; col. 58, lines 20-50); and employing information of said event to protection of said confidential (Ibid); said assessment identifying at least one policy (col. 43, line 55 – col. 44, line 15); and wherein in the event of two or more conflicting policies are found, a strictest one of the policies is identified and used (Ibid).

Although Ginter appears to disclose the use of identifiers from a content identifier database to identify protected information items (such as traveling objects: see col. 138, lines 43-62; and col. 305, line 45 – col. 306, line 5), Ginter does not explicitly disclose the use of statistical analysis in the process. However, Gilmour discloses a general technique for data management using statistical analysis with a number of identifiers to determine within a given confidence level if confidential information is present (the second matching step of col. 2, lines 20-50; identifiers at col. 13, lines 15-25; more detail at col. 21, lines 10-50). The claims are thus obvious because the ability to use statistical analysis to identify confidential data was a technique that was within the capabilities of one of ordinary skill in the art, in view of its teaching for improvement in similar situations.

Regarding claim 108:

Ginter further discloses handling an event (Ibid), said event being designated as directing information protection (Ibid), and employing said information protection technique in reaction to said event (Ibid).

Regarding claim 109:

Ginter further discloses wherein said event comprise any of: loading a local operating system, loading an application, user action, presenting a specific information into the system, an event generated by another system, suspicious activity, operating system time event, and a network time event (e.g. a user requesting to access protected content: col. 58, Ibid).

Regarding claim 123:

Ginter further discloses wherein said client software is operable to check that it is connected to a predetermined server before decrypting a file that comprise said protected information only while connected to at least one server (col. 305, lines 15-25).

Regarding claim 124:

Ginter further discloses wherein said servers enforce a policy with respect to said protected information, and wherein said policy comprises a set of restrictions regarding the usage of the said protected information (col. 341, lines 1-25).

Regarding claim 129:

Ginter further discloses wherein said software is operable to automatically add information to said protected information in accordance with said policy (col. 32, 25-35).

Regarding claims 147 and 148:

Ginter further discloses wherein controlling a user's action comprises at least one of preventing said action, monitoring said action, or logging said action (col. 303: 3-20).

6. Claims 1-61, 63-80, 107-130, and 147-149 are also rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter in view of Gilmour, and further in view of Albert et al. (U.S. Patent Publication 2003/0177389).

Regarding claims 1-61, 63-80, 107-130, and 147-149:

These claims are rejected for substantially similar reasons as discussed *supra*; however, it is observed that Albert explicitly teaches wherein when two or more security policies conflict with each other, as a general rule one should apply the most restrictive policy (paragraphs 0049-0059); per claim 149, this can be accomplished via a union of the respective policies (Ibid, particularly paragraphs 0053-0059). It would have been immediately obvious to one of ordinary skill in the art to ensure the most restrictive security policy applies when there exists any conflict, as one of ordinary skill in the art would have had good reason to pursue the known options within one’s grasp. If erring on the side of caution [e.g. a more restrictive policy] would lead to success, then the invention would be the result not of innovation but of ordinary skill and common sense.

7. Claims 107-109 are also rejected under 35 U.S.C. 103(a) as being unpatentable over "Java Security: How to Install the Security Manager and Customize Your Security Policy" (hereinafter, "Venners") in view of Gilmour in view of Albert.

Regarding claim 107:

Venners discloses a method for computer workstation based information protection comprising: detecting an event at said workstation, said event being associated with content (pages 1-2, "The Security Manager and the Java API"); directing handling of said event (Ibid); and employing information protection based on an assessment of an importance of said event to protection of information indicated as requiring protection technique (Ibid; cf. page 3, "Security beyond the architecture"), with Venner's security assessment identifying at least one policy (Ibid).

Although Venners discloses managing file access (page 2, last two bullet points on the first list therein), it appears to be silent regarding managing file access on the basis of using statistical analysis to identify confidential information. However, Gilmour discloses a general technique for data management using statistical analysis with a number of identifiers to determine within a given confidence level if confidential information is present (the second matching step of col. 2, lines 20-50; identifiers at col. 13, lines 15-25; more detail at col. 21, lines 10-50). The claims are thus obvious because the ability to use statistical analysis to identify confidential data was a technique that was within the capabilities of one of ordinary skill in the art, in view of its teaching for improvement in similar situations.

Although neither Venners nor Gilmour explicitly disclose wherein in the event of two or more conflicting policies being found, identifying and using the strictest one; nevertheless Albert confirms that this is common knowledge in the art (paragraphs 0049-0059). It would have been immediately obvious to one of ordinary skill in the art to ensure the most restrictive security policy applies whenever there exists any conflict, as one of ordinary skill in the art would have had good reason to pursue the known options within one's grasp. If erring on the side of caution [e.g. a more restrictive policy] would lead to success, then the invention would be the result not of innovation but of ordinary skill and common sense.

Regarding claim 108:

Venners further discloses handling an event, said event being designated as directing information protection (pages 1-2, "The Security Manager and the Java API"); and employing a said information protection technique in reaction to said event (Ibid).

Regarding claim 109:

Venners discloses wherein said event comprise any of: loading a local operating system, loading an application, user action, presenting a specific information into the system, an event generated by another system, suspicious activity, operating system time event, and a network time event (bulleted list on page 2).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- U.S. Patent Publication 2003/0051165 to Krishnan
- U.S. Patents 7,546,629 (Albert); 7,516,475 (Chen); 7,373,659 (Vignoles); 7,140,035 (Karch); and 6,854,016 (Kraenzel)
- “Principle of Least Privilege” and “Executing Java Programs Securely”

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 9:30am - 6:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
10/25/10
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435